

Tel : +27 12 341 9638 / 9651  
Fax : +27 12 341 5938

Private Bag X08 | Arcadia | 0007  
523 Church Street | 5<sup>th</sup> Floor | Provisus Building | Arcadia



## **ANNEXURE A**

### **APPOINTMENT OF A SERVICE PROVIDER FOR PENETRATION TESTING SERVICES FOR A PERIOD OF THREE (3) YEARS**

#### **1. PURPOSE**

The Pan South African Language Board (PanSALB) is hereby requesting proposals for Penetration Testing Services for a period of thirty-six months which will be contacted twice a year.

#### **2. INTRODUCTION AND BACKGROUND**

Pan South African Language Board is an entity of government under the Department of Sport, Arts and Culture, which promotes and supports the development of languages within South Africa. The Board was established by national legislation with the exclusive mandate to promote and create conditions for the development and use of all official languages of the Republic of South Africa, including the KHOI, Nama and San languages, and the South African Sign language.

In order to perform the above-mentioned responsibility, PanSALB utilizes Information and Communication Technology as the platform to manage and provide access to its systems and communicate with its stakeholders. These ICT systems and infrastructure are subject to cyber-attacks and need to be secured both internally and externally.

The main reason for such protection is in line with legislation relating to the POPI Act as well as common law principles of information privacy, confidentiality, and accessibility. The other reason is mainly to protect the PanSALB data and information assets from any harm or unauthorized access by both internal staff and external people who may have malicious intent to bring the organization down by means of Denial of Service (DoS).

PanSALB would like to do offensive security and be proactive in uncovering cyber threats and vulnerabilities before cybercriminals do

#### **3. THE PURPOSE OF THIS RFQ**

This RFQ seeks to appoint a suitably qualified service provider with ICT Security expertise to perform vulnerability assessment and penetration testing not limited to the following:

- Penetration Testing and vulnerability assessment service twice a year for both internal and external ICT environments related to PanSALB including the reporting services with recommendations;

The purpose is to manage cyber threats (both internal and external) against the PanSALB's resources and ensure that it addresses the continually developing cyber threat environment for all of PanSALB sites. The output of this bid is to provide data security and threat protection to the PanSALB sites, both internally and externally and protection against potential harmful software and human-related attacks against the PanSALB's data.

#### **4. SCOPE OF WORK, SERVICES AND PRODUCTS REQUIRED**

The service provider is expected to provide the following services bi-annually for the duration of the contract:

4.2 Provide a service to identify vulnerabilities on the PanSALB systems and ICT Infrastructure twice a year through:

- The Internal vulnerability assessment services
  - Internal LAN IPs which include servers, switches, intranet, workstations, printers
  - WiFi security testing
  - Reporting services which include the remedial plans
- The External vulnerability assessment services
  - External IP Addresses IPs which includes (website, firewall, and public-facing applications)
  - Reporting services which include the remedial plans
- Penetration Testing
  - Gray-box Internal penetration testing
  - Black-box External penetration testing
  - Reporting services which include the remedial plans

4.3 Provide executive reports showing overall risk score based on the severity of the aggregated identified vulnerability.

4.4 Provide detailed technical reports showing vulnerabilities, risk scores and remedial solutions.

Suggested prioritized remedial action implementation approach and plan to rapidly mitigate all identified vulnerabilities.

#### **Exclusions**

Exclusions for the required penetration test - **No DoS attacks** that could affect the services.

#### **5 REQUIRED DELIVERABLES**

The following are the deliverables for this RFQ :

A Penetration Testing and vulnerability assessment and penetration service with reporting service and clear recommendations on the remedial actions to be taken.

#### **6 SUPPORT:**

The successful service provider is required to support PanSALB with remediation advisory services for the duration of the contract.

#### **7. TIME FRAMES FOR DELIVERY OF WORK**

The implementation phase is estimated to be completed within thirty (30) days from the start date occurring bi-annually. The support and maintenance service will continue for a period of thirty-six (36) months.

ELEMENT	FUNCTIONALITY EVALUATION		FUNCTIONALITY WEIGHT	TOTAL SCORE
<b>Proposed Technical approach and methodology of the bidder:</b>	<b>Rating out of 5</b>	<b>Evaluation criteria</b>		
<p>The service provider to submit a detailed project implementation plan based on the timelines provided includes: -</p> <ul style="list-style-type: none"> <li>✓ All tasks and activities</li> <li>✓ Resources;</li> </ul> <p>With the implementation phase taking thirty (30) days from the date of appointment <b>(20 Points)</b></p>	0	Project Implementation plan not submitted/Project implementation plan submitted but does not cover the full scope of work/Proposal indicates implementation taking more than forty (40) days from date of appointment.		
	3	Project Implementation that includes the full scope of work, required timeframes, and deliverables taking more than thirty (30) days from the date of appointment.		
	5	Project Implementation that includes the full scope of work, required timeframes, and deliverables and can be delivered within thirty (30) days from the date of appointment		
<b>Suitability of the bidder:</b>	<b>Rating out of 5</b>	<b>Evaluation criteria</b>		
<ul style="list-style-type: none"> <li>• The Service Provider is to indicate a minimum of three (3) projects where a similar assignment of penetration testing services was rendered.</li> </ul> <p>Service providers are required to submit reference letters on the client's letterhead with contactable references of similar services <b>(30 Points)</b>.</p>	0	The service provider has not undertaken a project where a similar assignment of vulnerability assessment and penetration testing services were rendered/service provider submitted less than three (3) reference letters		
	3	The service provider has undertaken a minimum of two (2) projects of vulnerability assessment and penetration testing services and two (2) reference letters on the client's letterhead with contactable references of similar services were submitted		
	5	Bidder has undertaken three (3) or more projects of vulnerability assessment and penetration testing and three (3) or more reference letters on the client's letterhead with contactable references of similar services were submitted		

ELEMENT	FUNCTIONALITY EVALUATION		FUNCTIONALITY WEIGHT	TOTAL SCORE
<b>Suitability of the proposed team:</b>	<b>Rating out of 5</b>	<b>Evaluation criteria</b>		
The service provider is to submit a comprehensive CV of the team leader demonstrating a minimum of ten (10) years of experience in performing vulnerability assessment and penetration testing services <b>(30 Points)</b> .	0	CV of the team leader not submitted/ CV of the team leader demonstrates less than five (5) years of experience performing vulnerability assessment and penetration testing services.		
	3	CV of the team leader submitted demonstrating a minimum of five (5) years of experience in performing vulnerability assessment and penetration testing services.		
	5	CV of the team leader submitted demonstrating a minimum of ten (10) years of experience or more in performing vulnerability assessment and penetration testing services.		
The service provider to submit a team comprising the team leader and a minimum of one (1) additional team member to collectively possess qualifications in the following:  (1) OSCP, (2) CPTE, (3) CISM, (4) CEH  <b>NB.:</b> It is to be noted that it is not required for each person on the team to have all certificates, but for the team as a collective to have a minimum of three certificates. Proof of these certificates to be submitted with the proposal. Proposals without the required certificates will be scored according to the rating scale <b>(20 Points)</b> .	0	The service provider did not submit qualification certificates for the proposed team members/ Service provider submitted less than two (2) required qualification certificates		
	3	The Service provider submitted two (2) certificates for the proposed team members required qualification certificates		
	5	The Service provider submitted a minimum of three (3) certificates for the proposed team members' required qualification certificates		
<b>TOTAL POINTS</b>			<b>100%</b>	

Bidders to meet the minimum functionality requirement of 70%. Bidders who do not meet this minimum requirement will be eliminated from further evaluation and bidders who meet the minimum threshold will be shortlisted for further evaluation.